



**Department of Economic Security**  
Information Technology Standards

Title: 1-38-0016 Media Sanitizing/Disposal Policy

<i>Subject:</i> This policy defines DES media sanitizing and disposal requirements.	<i>Effective Date:</i>  05/11/04	<i>Revision:</i>  1.2
---	--	-----------------------------

## 1. Summary of Policy Changes

- 1.1 01/06/05 – Major changes submitted by DTS ISA, moving responsibility for cleaning to DTS.
- 1.2 06/21/05 – Revised with more stringent sanitization procedures.

## 2. Purpose

- 2.1 This document addresses policy concerning Media Sanitizing/Disposal Policy defines requirements for appropriate disposal of data stored on IT media devices.

## 3. Scope

- 3.1. This policy applies to all DES administrative elements, divisions and programs, boards and commissions.
- 3.2. This policy applies to all authorized DES computer system users, defined as every DES employee, contractor, temporary staff member, or any other person with DES management's approval to access DES computing systems.  
This policy applies to all data and hardware in use within DES. Data in electronic form may reside in many environments including mainframe computers, mid-range computers, LANs, and WANs inside of DES.

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

## 4. Responsibilities

- 4.1. The DES Director, Deputy Directors, Associate Directors, and Assistant Directors are responsible for enforcing this policy.
- 4.2. The DES Director or his designee, is responsible for:
  - 4.2.01. Archiving Records, Acceptable Methods for Disposal of Data, Destruction of Storage Devices, and Assurance of Sensitive Data Removal.
  - 4.2.02. Providing the technological means for implementing those policies and procedures.
  - 4.2.03. Providing the means enforcing the policies and procedures.
- 4.3. The DES CIO is responsible for implementing, supporting, and maintaining appropriate hardware, software, staff, and infrastructure to support adherence to this policy.

4.4.The DTS and DES IT Managers are responsible for monitoring compliance of sanitizing and appropriate disposal of hardware.

## **5. Definitions and Abbreviations**

### **5.1. Definitions**

### **5.2. Abbreviations**

## **6. POLICY**

**6.1.General Policy Statement** – Media Sanitizing/Disposal Policy defines requirements for appropriate disposal of IT devices (servers, storage, or clients), network components, operating system or application software, or storage media to prevent unauthorized use or misuse of stored information.

The following standards provide requirements that ensure secure and appropriate disposal of information technology (IT) devices, network components, operating system or application software, and storage media belonging to DES to prevent unauthorized use or misuse of State information. This can include, but is not limited to: magnetic tapes, floppy disks, removable disk drives, optical disks, non-volatile memory devices (including memory sticks and cards or USB memory storage and Personal Digital Assistants (PDAs). Storage devices currently available but not used by DES or that become available in the future due to new technology are also covered.

**6.2.Archiving Records:** Any IT devices (servers, storage, clients), network components, operating system or application software, or storage media containing public/official records shall have the final disposition of those records established with State Library, Archives, and Public Records (SLAPR) before being disposed of through Arizona Department of Administration, Management Services Division, Surplus Property Management Office (SPMO) or provided to another State organization for “reuse.”

### **6.3. Responsibility for Sanitization:**

#### **6.3.01. Surplus Computers and Servers**

- 6.3.01.1. All computers and servers that going to State surplus must go through DES surplus. The surplusing Division will contact DES surplus to retrieve the designated equipment.
- 6.3.01.2. DES Surplus will utilize a third party partner (Currently, Arizona Industries for the Blind (AIB)) to sanitize any equipment discussed in section 6.1.
- 6.3.01.3. AIB will follow all policies and procedures outlined in this policy and in the Service Level Agreement between AIB and DES.
- 6.3.01.4. All sanitized equipment will then go to State Surplus as outlined in the SLA with a “Letter of Certification” from AIB.
- 6.3.01.5. The Information Security Administration is responsible for periodic auditing and monitoring AIB to ensure that all stipulations of the SLA are met.

### **6.3.02. Transfer of Computers and Server**

- 6.3.02.1. All Divisions will train and certify designated personnel on how to sanitize hard drives. A list of personnel who have been trained will be provided to ISA by each Division and updated on a quarterly basis.
- 6.3.02.2. When computer equipment is transferred to another Division or Program outside of their Division (still internal to DES), it must be sanitized to the standard discussed in section 6.4.
- 6.3.02.3. The accepting unit of the equipment must only receive said equipment if it is accompanied by a certification form from the transferring unit. This documentation must be kept for 3 months after the receipt of the equipment.

**6.4. Acceptable Methods of Disposal:** Before a disk device is disposed of through SPMO, data stored on the device shall be deleted in a manner that renders it unrecoverable via ISST. DES shall use DOD approved software that erases data from hard drives seven layers down to make the data unrecoverable. Recommended software to do this: Boot and Nuke (a freeware program). If the disk may contain confidential or private information, then the disk should be degaussed and rendered unusable. Physical destruction of the disk may also be used in this scenario.

**6.5. Portable media** (diskettes, tapes, CD-ROMs): may be destroyed by crushing, incinerating, shredding, or melting. If they are to be reused, portable media must be erased using a secure erase program.

**6.6. Unacceptable Methods of Disposal:** Such methods shall not place undue cost overhead upon DES nor place employees at physical risk. Use of dangerous equipment, toxic, flammable or dangerous substances shall not be used to accomplish secure disposal.

**6.7. Repairing media devices:** Sometimes media cannot be repaired in house and may have to be sent to the vendor for repair or to be swapped for a warranty replacement part. Before a hard drive is sent to a vendor for exchange or repair the hard drive should be cleaned or degaussed. If the hard drive is not accessible e.g. damaged or has an electronic problem, management must make a determination whether or not to replace instead of repairing the piece of equipment. The inaccessible piece of equipment needing repair must be destroyed.

**6.8. Assurance of Sensitive Data Removal:** The agency shall use AIB to effect the removal of any sensitive data from IT devices. All devices that have been sanitized must be inventoried and documented. This documentation will need to be retained for six years. The documentation must clearly identify the asset or media to be disposed and include the dates and means of sanitization, authorization, and method of disposal.

## **7. Implications**

7.1. None.

## **8. Implementation Strategy**

8.1. All DES divisions and programs shall comply with this policy.

## **9. References**

- 9.1. A. R. S. § 41-621 et seq., “Purchase of Insurance; coverage; limitations, exclusions; definitions.”
- 9.2. A. R. S. § 41-1335 ((A (6 & 7))), “State Agency Information.”
- 9.3. A. R. S. § 41-1339 (A), “Depository of State Archives.”
- 9.4. A. R. S. § 41-1461, “Definitions.”
- 9.5. A. R. S. § 41-1463, “Discrimination; unlawful practices; definition.”
- 9.6. A. R. S. § 41-1492 et seq., “Prohibition of Discrimination by Public Entities.”
- 9.7. A. R. S. § 41-2501 et seq., “Arizona Procurement Codes, Applicability.”
- 9.8. A. R. S. § 41-3501, “Definitions.”
- 9.9. A. R. S. § 41-3504, “Powers and Duties of the Agency.”
- 9.10. A. R. S. § 41-3521, “Information Technology Authorization Committee; members; terms; duties; compensation; definition.”
- 9.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
- 9.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
- 9.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
- 9.14. Arizona Administrative Code, Title 2, Chapter 15, Article 3 Materials Management, “Disposition.”
- 9.15. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
- 9.16. Statewide Information Technology Policy P100.
- 9.17. Statewide IT Security Policy P800.
- 9.18. State of Arizona Target Security Architecture

## **10. Attachments**

10.1 None

## **11. Associated Government Information Technology Agency IT Standards or Policies**

11.1 None

## **12. Review Date**

12.1 This document will be reviewed twelve (12) months from the original adoption date, and every twelve months thereafter.